AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Google account ian.a.matteson@gmail.com

Case No. MJ17-5217

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Google account ian.a.matteson@gmail.com as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252(a)(4)(B)	Access with Intent to View Child Pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christian A. Huntzinger, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: December 13, 2017

Judge's signature

City and state: TACOMA, WASHINGTON

THERESA L. FRICKE, U.S. MAGISTRATE JUDGE
Printed name and title

2017R01183

ATTACHMENT A

Account(s) to be Searched

The electronically stored data related to, and associated with Google account:

ian.a.matteson@gmail.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

I. Section I - Information to be disclosed by Google for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Google Chrome Browser history including but not limited to all search engine searches, including Bing Images and Google Images, as well as all URLs accessed (whether direct typed or linked from a search engine or other referring page). This information should include Bing or Google search suggestions and any searches that were typed by the user but that did not render results. This history should include date and time stamps associated with this activity.

b. List of devices that have accessed this user's Google account including any and all identifiers of the device such as Universal Unique Identifier (UUID), IMEI, operating system, etc.

c. List of software applications which have been utilized to access Google Chrome or other websites/URLs.

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. The types of service utilized;

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. 2252(a)(4)(B) (access with intent to view child pornography) that occurred between April 1, 2016, and the present, including,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All profile information or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

b. All Google Chrome Browser history related to depictions of minors engaged in sexually explicit conduct (whether direct typed or linked);

c. List of devices that have accessed this user's Google account including any and all identifiers of the device such as UUID, IMEI, operating system, MAC address, etc.

d. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number; and

e. Any and all other log records, including IP address captures, associated with the specified account.

Notwithstanding the criminal offenses defined under 18 U.S.C. § 2252 and 2252A or any similar criminal offense, Google shall disclose information responsive to this warrant by mailing it to Naval Criminal Investigative Service, Attn: Special Agent Christiana Huntzinger at 3405 Welles Street, Suite 1, San Diego, CA 92136.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Special Agent Christiana Huntzinger, upon being duly sworn do hereby state that the following is true to my knowledge and belief:

1. I am a Special Agent with the Naval Criminal Investigative Service and have been for over thirteen years. I am currently assigned to the Cyber Operations, San Diego Field Office, and have worked as a full time or affiliate member of the San Diego Internet Crimes Against Children (ICAC) task force for my entire career. I specialize in investigating criminal violations relating to online child exploitation, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography in violation of 18 U.S.C. §§ 2251, 2252 and enticement of minors in violation of 18 U.S.C. § 2422(b). I have participated in the execution of hundreds of state and federal search warrants, probation searches, and U.S. Navy Command Authorized searches, which involved child exploitation and/or child pornography offenses. Additionally, I have viewed hundreds of thousands of images and videos of all types of child pornography. I have a Bachelor of Arts degree in Criminology and a Masters Degree in Forensic Science. In addition to completing the basic requirements to be an NCIS agent, I have received over 900 hours of training regarding cyber and child pornography investigations, including the preservation of digital evidence.

2. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, CA, 94043. The information to be searched is described in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

to the government copies of the information (including Google Chrome browser history) as described in Section I of Attachment B and permit government-authorized personnel to review that information to locate the items described in Section II of Attachment B.

3. This affidavit is based upon information I have gained through training and experience, as well as upon information related to me by other individuals, including law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known concerning this investigation but have set forth only the facts that I believe is necessary to establish probable cause to believe that evidence relating to violations of Title 18, United States Code §2252 is located at the address described in Attachment A.

4. Based upon the following information, I believe there is probable cause to conclude that currently located within the location further described in Attachment A is is evidence, fruits, and instrumentalities of the offense of access with intent to view child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and the attempt to do so, as more particularly described in Attachment B.

BACKGROUND ON GOOGLE, BING, AND MILITARY COMPUTER NETWORKS

5. In my training and experience, I have learned that Google is a technology company that offers a variety of Internet-related services and products. Google is most commonly known as a search engine, however, Google also offers cloud storage (Google Drive), email (Gmail), social networking (Google+), and photo organizing (Google Photos). Google is also responsible for the development of the Google Chrome web browser.

6. Google's Chrome web browser is an application that allows a user to access the Internet. Just as with any other browser, Google Chrome allows the user to type a URL directly to access a website or use a search engine to locate a desired website. Relevant here are the Google and Bing search engines. Both of these search engines allow the user to narrow the scope of a search to a particular type of material such as maps, images, etc.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

7. Results from Google Search and Bing Search are populated by data from the Internet that have been indexed. Both Google and Bing have automated programs called "bots" or "crawlers" that locate web URLs and index the information for retrieval by users of the search engine. Any user with Internet access can use a web browser and search engine to locate indexed web pages. The method of crawling and indexing is complicated and based on proprietary coding. Search results are largely based on metadata or tags associated with the image, such as the image's title. For example, a Bing Images search for "sunset" will typically render pictures of a sunset but may also render images of a t-shirt showing a sunset that is titled, "sunset t-shirt.jpg"

8. When a user logs into his/her Google account (such as Gmail) via Google Chrome and then accesses the web, his/her personal browsing data are saved on Google's servers and synced with that account. This saved information includes browsing history, bookmarks, tabs, and browser settings. The Google Chrome browser is defaulted to automatically sync the browsing history, bookmarks, tabs, and browser settings to each device when a user logs in. If set to the default, these settings are therefore automatically loaded anytime the user signs into Google on other computers and devices. The user can customize what information is synchronized, however, the default method is to store all information as listed above.

9. Users often stay logged into their Google account even after the browser is closed and then re-launched. Logging out of Google takes an affirmative action to click on an icon and select "log out." For this reason, many users stay logged into their Google account constantly. If a user is logged into Google and accesses a webpage, Google stores this information as associated with the account. If a user accesses Bing or Google search engines, Google stores this information associated with their account.

10. To obtain a Google account, a subscriber must register with Google and provide certain personally identifying information, which can include the subscriber's name, phone number, address, alternative email addresses, etc. Such information may constitute evidence of the crimes under investigation because the information can be used to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

identify the account's user or users and establish who has dominion and control over the account. When an individual is logged in to his/her Google (Gmail) account, Google logs the IP address associated with the Internet access of the computer or phone accessing the account. An IP address is a unique address expressed numerically, and is unique to a particular computer during an online session. IP addresses are assigned by the Internet Service Provider and provide a unique identifier making it possible for communication between network equipped device, including computers. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different number to a network equipped device every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's device a particular IP address which is used each time the computer accesses the Internet. Obtaining the IP addresses that have been utilized to log into a particular Google/Gmail account identifies the Internet Service Provider that owns and has leased that address to its customer. Subscriber information for that customer then can be obtained using appropriate legal process in order to further identify where the IP address originates from and possibly identify the user.

11. The Navy Marine Corps Intranet (NMCI) is the primary network infrastructure allowing access to the Internet on Department of the Navy (DON) facilities and bases in the continental United States. NMCI is responsible for providing DON personnel with computers and unclassified Internet access in order to carry out their official duties. NMCI Internet access is intended to be used for official business purposes.

12. NMCI's network is referred to as a "bannered" network because a banner containing a legal notice is displayed and must be acknowledged by the user before access is granted. The legal notice states, "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following . . . The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations."

13. DON personnel are allowed, as part of their official duties, to access the Internet via the NMCI network. When a user visits a particular page, the request is funneled through a proxy, which serves as an intermediary between the user and the Internet. The proxy is a piece of proprietary software that sits on the network and categorizes the content of a domain/websites. A determination of category is based on a series of complicated programmatic factors such as the history of the domain, keywords, etc. For example, if a user attempts to access CNN, the proxy will categorize the content as something similar to: News/Marketing/Business. The proxy is also configured to allow the user to access certain categories of content but not others. For example, the user would be allowed to access CNN because it is not a blocked category. However, if a user attempts to access a website containing child pornography, the user will not be able to view the website and will instead receive a notification that the website they are attempting to access is blocked.

14. NMCI logs all Internet activity for a period of time, including attempts to access websites containing illegal material such as child pornography. These logs are routinely provided to NCIS and reviewed for investigative consideration. These logs contain the name and user credentials of the user, the location where the activity originated (base name, building number, etc.), the website the user attempted to access, and any website that referred the user to the blocked website, such as a search engine. Commonly, users will conduct a search on Bing or Google images, review the results, and then attempt to access the source image on the linked webpage. As would be expected, child pornography sites are blocked on this network. However, the results of images on search engines are allowed. The Bing Images or Google Images queries can be duplicated to determine the type of material the user was viewing.

15. At the request of NCIS, NMCI also has the ability to conduct a remote "profile data pull" for any NMCI user. This data pull consists of a logical extraction of the government computer(s) associated with a particular user account. This profile pull is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

conducted remotely, burned to disk or placed onto a hard drive, and can be provided to NCIS. Because this information comes from the bannered, government network and government equipment, it is reviewed without additional search authority. Because the profile pull is only a logical extraction, it does not include deleted items or items in unallocated space.

THE INVESTIGATION

16. Between May 1 and May 9, 2017, I reviewed Internet browsing activity (proxy logs) for NMCI computer account NADSUSWE\ian.matteson, which is associated with a civilian Navy employee named Ian MATTESON. This browsing history contained URLs indicative of child sexual exploitation material. The logs covered the period from April 7, 2016, through April 20, 2017.

17. These logs showed hundreds of apparent attempts by MATTESON to access websites categorized by the proxy as having content: Child Pornography or Pornography; Malicious Sources/Malnets. These access attempts were primarily the result of Bing Images searches conducted by MATTESON. As noted above, MATTESON would have been able to view the search results generated by these searches. The log entries described above resulted from attempts by MATTESON to access some of these results by clicking on one of the images displayed and then having his access blocked by the network filters. As part of this investigation, I replicated several of the searches conducted by MATTESON. It should be noted that the replicated searches did not occur at the same time as MATTESON conducted them, and I therefore cannot say with certainty that the results visible to me were identical to those seen by MATTESON. Although many of the search terms used by MATTESON did not on their face appear to be connected to child pornography, the search results I obtained contained a significant number of suspected child pornography images and images of child erotica. Though these search results also contained images of apparent adult pornography. I describe several of these searches below.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. On May 8, 2017, I duplicated a Bing Images search for "Converting Onion Tag Cam" conducted by MATTESON on April 20, 2017. Among the search results were several images of what appeared to be prepubescent minors engaged in various sex acts.

19. On May 8, 2017, I duplicated a Bing Imags search for "Pimpandhost Converting to Mrvine" conducted by MATTESON on March 9, 2017. The results show a gallery of images depicting child pornography and child erotica. Most of the images show a series of frames from a movie. These include a series of images/frames showing adult fingers pulling open the genitals of a very small female child. There are also images that show a child with a piece of tape over her mouth being raped by an adult male.

20. On May 8, 2017, I duplicatd a Bing Images Search for "Converting Tag Onionib" conductd by MATTESON on March 9, 2017. The search produced a gallery of images, including images of child pornography. Among these was an image depicting an infant female with red marks around her vagina and anus.

21. MATTESON is a Navy civilian employee who works as a System/Mechanical Engineer at the Navy Underwater Warfare Center (NUWC), Keyport, Washington. Accordingly to military personnel records, MATTESON resides in Silverdale, Washington.

22. At my request, NMCI conducted a profile data pull of MATTESON's account. This data pull was then forensically imaged and reviewed by NCIS. Among other things, the review revealed MATTESON sent emails from his official government account to ian.a.matteson@gmail.com. The review also uncovered several emails from Google (no-reply@accounts.google.com) that stated, "New sign-in from Samsung Galaxy S6 Hi Ian, Your Google Account ian.a.matteson@gmail.com was just used…"

23. This examination also uncovered numerous search queries from Bing Images, consistent with the search terms listed above and identified in the proxy logs. The searches were located at the following file path: ian.matteson\WLKYPT005606\AppData\Local\Google\Chrome\User Data\Default\Favicons. This file path indicates MATTESON use the Google Chrome browser to access the web and conduct the searches.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

24. Finally, this profile review uncovered several images of suspected child pornography in a cache file associated with the Google Chrome web browser at the following path: ian.matteson/WLKYPT005606/AppData/Local/Google/Chrome/User Data/Default/Cache. I describe several of these images below:

f_00a1a.jpg: This image depicts a prepubescent female lying nude on a leopard-print blanket. She is lying on her left side with her right leg up, exposing her genitals to the camera. Based on the lack of pubic hair and breast/muscle development, as well as her overall appearance, I estimate she is between nine and twelve years old.

f_0009e8.jpg: This image depicts a prepubescent female lying on her back on a red and white checkered blanket. Other than a white hat on her head, she is nude. A nude, adult female is hovering over the child and painting around the child's nipple. Based the child's lack of pubic hair and breast/muscle development, her size in comparison to the adult female, and her overall appearance, I estimate she is between nine and twelve years old.

f_00096a.jpg: This image depicts a pubescent female sitting with her legs open and her genitals visible to the camera. Another female is lying on the seated female. She also appears to be nude, though her entire body is not visible. The word "SAMPLE" is printed across the front of the picture in large, white letters. Based on her lack of pubic hair and breast/muscle development, as well her overall appearance, I estimate the pubescent is between ten and thirteen years old.

f_000971: This image depicts a pubescent nude female child lying on a bed with a blue patterned bedspread. She is lying on her side and looking at another child, who is lying on his/her left side and looking at the camera. The second child's genitals are not entirely visible, so it is unclear if this child is male or female. This child is looking at the camera and smiling. Based on their lack of muscle development and overall appearance, I estimate that the two children depicted in this image are between twelve and fifteen years old.

25. The metdata associated with the four images described above show that they were downloaded to MATTSON's computer at around noon on May 2, 2017. Although these files were stored automatically by the Google Chrome browser, they would not be present unless they have been visible to the computer while accessing the internet.

26. Hardcopies of the four images described above have been placed in an envelope that is marked as Exhibit 1. Exhibit 1 will be made available to the reviewing

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

magistrate judge upon presentation of this search warrant application. After the presentation, Exhibit 1 will not be filed with the Court but will instead remain in the custody of law enforcement and will be retained by law enforcement to be made available should Exhibit 1 be relevant to a future legal proceeding.

CHILD EXPLOITATION INVESTIGATIONS

27. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly. They also may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an Internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography. distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

28. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification.

I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

29. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that MATTESON likely has a sexualized interest in children and depictions of children and that evidence of access with intent to view child pornography is likely to be found in the information associated with the Google account ian.a.matteson@gmail.com sought in this application.

PAST EFFORTS TO OBTAIN THIS EVIDENCE

30. This evidence, in part, has been provided to me via the NMCI proxy logs, and the NMCI profile data pull. The proxy logs are limited in that they only capture activity that is categorized by an automated program as being unauthorized to access. The proxy also cannot log details regarding encrypted traffic. The NMCI data profile pull is only a logical extraction of the user's activity and does not see deleted data, including deleted Internet access logs or deleted cookies. Obtaining this evidence directly from Google will provide the most complete activity of this user's online activity via Google Chrome. No previous efforts have been made to obtain this evidence from Google.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

31. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit **Google** and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to **Google** with direction that it identify the **Google** account described in Attachment A to this affidavit, as well as other subscriber and log records associated with the accounts, as set forth in Section I of Attachment B to this affidavit.

32. The search warrant will direct Google to create an exact copy of the specified account and records.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

33. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

34. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

35. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of e-mail communications, chat logs and documents, that identify any users of the subject account and e-mails sent or received in temporal proximity to incriminating e-mails that provide context to the incriminating communications.

CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the court is "a district court of the United States . . . that - has jurisdiction over

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the offense being investigated." (18 U.S.C. § 2711(3)(A)(i).) Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachment B, and specifically to seize all of the data, documents and records that are identified in Section II of that same Attachment.

Christiana Huntzinger, Special Agent
Naval Criminal Investigative Service

Subscribed and sworn to before me this 13th day of December, 2017. In addition to this affidavit, I have reviewed the images contained in Exhibit 1 to this affidavit. Upon reviewing them, the envelope containing them was sealed, and I affixed my signature across the seal.

Theresa L. Fricke
THERESA L. FRICKE
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Account(s) to be Searched

The electronically stored data related to, and associated with Google account:

ian.a.matteson@gmail.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

I. Section I - Information to be disclosed by Google for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Google Chrome Browser history including but not limited to all search engine searches, including Bing Images and Google Images, as well as all URLs accessed (whether direct typed or linked from a search engine or other referring page). This information should include Bing or Google search suggestions and any searches that were typed by the user but that did not render results. This history should include date and time stamps associated with this activity.

b. List of devices that have accessed this user's Google account including any and all identifiers of the device such as Universal Unique Identifier (UUID), IMEI, operating system, etc.

c. List of software applications which have been utilized to access Google Chrome or other websites/URLs.

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. The types of service utilized;

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. 2252(a)(4)(B) (access with intent to view child pornography) that occurred between April 1, 2016, and the present, including,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All profile information or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

b. All Google Chrome Browser history related to depictions of minors engaged in sexually explicit conduct (whether direct typed or linked);

c. List of devices that have accessed this user's Google account including any and all identifiers of the device such as UUID, IMEI, operating system, MAC address, etc.

d. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number; and

e. Any and all other log records, including IP address captures, associated with the specified account.

Notwithstanding the criminal offenses defined under 18 U.S.C. § 2252 and 2252A or any similar criminal offense, Google shall disclose information responsive to this warrant by mailing it to Naval Criminal Investigative Service, Attn: Special Agent Christiana Huntzinger at 3405 Welles Street, Suite 1, San Diego, CA 92136.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [**Google**], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [**Google**]. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[Google]**, and they were made by **[Google]** as a regular practice; and

b. such records were generated by **[Google's]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[Google]** in a manner to ensure that they are true duplicates of the original records; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. the process or system is regularly verified by **[Google]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Account(s) to be Searched

The electronically stored data related to, and associated with Google account:

ian.a.matteson@gmail.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

I. Section I - Information to be disclosed by Google for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Google Chrome Browser history including but not limited to all search engine searches, including Bing Images and Google Images, as well as all URLs accessed (whether direct typed or linked from a search engine or other referring page). This information should include Bing or Google search suggestions and any searches that were typed by the user but that did not render results. This history should include date and time stamps associated with this activity.

b. List of devices that have accessed this user's Google account including any and all identifiers of the device such as Universal Unique Identifier (UUID), IMEI, operating system, etc.

c. List of software applications which have been utilized to access Google Chrome or other websites/URLs.

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. The types of service utilized;

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. 2252(a)(4)(B) (access with intent to view child pornography) that occurred between April 1, 2016, and the present, including,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All profile information or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

b. All Google Chrome Browser history related to depictions of minors engaged in sexually explicit conduct (whether direct typed or linked);

c. List of devices that have accessed this user's Google account including any and all identifiers of the device such as UUID, IMEI, operating system, MAC address, etc.

d. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number; and

e. Any and all other log records, including IP address captures, associated with the specified account.

Notwithstanding the criminal offenses defined under 18 U.S.C. § 2252 and 2252A or any similar criminal offense, Google shall disclose information responsive to this warrant by mailing it to Naval Criminal Investigative Service, Attn: Special Agent Christiana Huntzinger at 3405 Welles Street, Suite 1, San Diego, CA 92136.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [**Google**], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [**Google**]. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[Google]**, and they were made by **[Google]** as a regular practice; and

b. such records were generated by **[Google's]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[Google]** in a manner to ensure that they are true duplicates of the original records; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. the process or system is regularly verified by **[Google]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970